Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO - Version 1.3 - Erstellt am 09.09.2026

Vertragsparteien

Verantwortlicher (nachfolgend „Auftraggeber")

Unternehmen	_____ (vom Salon-Kunden auszufüllen)
Ansprechpartner	_____
Anschrift	_____
E-Mail	_____

Auftragsverarbeiter (nachfolgend „Auftragnehmer")

Unternehmen	Marcus Euchner - Platrion
Anschrift	Lange Gasse 34, 72581 Dettingen an der Erms, Deutschland
E-Mail	info@platrion.de
Telefon	+49 157 73551423

1. Gegenstand und Dauer der Verarbeitung

(1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der im Hauptvertrag (Projekt- bzw. Servicevertrag) vereinbarten Leistungen. Soweit nicht abweichend vereinbart, umfasst dies insbesondere:

• Bereitstellung der SaaS-Plattform „SchnittBuch" zur Online-Terminbuchung für Friseure, Salons und vergleichbare Dienstleistungsbetriebe gemäß Hauptvertrag (SchnittBuch Start, SchnittBuch Komplett-Tarif) sowie den zugehörigen AGB § 21.

(2) Dauer: Für die Dauer des SchnittBuch-Nutzungsvertrags. Nach Vertragsende werden alle personenbezogenen Endkundendaten binnen 30 Kalendertagen gelöscht, Backups binnen weiterer 90 Tage.

(3) Die Verarbeitung erfolgt ausschließlich im Gebiet der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Eine Übermittlung in Drittländer erfolgt nur, wenn die besonderen Voraussetzungen von Art. 44 ff. DSGVO erfüllt sind.

2. Art und Zweck der Verarbeitung

Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag und umfassen insbesondere:

• Bereitstellung eines Online-Buchungssystems (SchnittBuch) für die Terminverwaltung des Salon-Kunden mit dessen Endkundinnen und Endkunden
• Speicherung der Termindaten und Stammkundenhistorie in einer eigens für den Salon-Kunden isolierten Mandanten-Datenbank
• Automatischer Versand von Buchungsbestätigungen und Erinnerungs-E-Mails an die Endkunden des Salon-Kunden über Resend (siehe § 6 Unterauftragsverarbeiter)
• Bereitstellung eines Salon-Admin-Dashboards mit Kalenderansicht und CSV-Export-Funktion
• Technischer Betrieb, Wartung, Sicherheits-Updates und Backup der Plattform (auf Servern in Frankfurt am Main)

3. Art der personenbezogenen Daten

Folgende Kategorien personenbezogener Daten werden verarbeitet:

• Stammdaten der Endkunden (Vorname, Nachname)
• Kontaktdaten der Endkunden (E-Mail-Adresse, Telefonnummer)

• Termindaten (Datum, Uhrzeit, gewählte Leistung, zugeordneter Mitarbeiter)
• Freitext-Notizen des Endkunden bei der Buchung (z. B. Farbwunsch, Allergien) – nur soweit vom Endkunden freiwillig angegeben
• Buchungshistorie zur Wiedererkennung von Stammkundinnen
• IP-Adresse und Zeitstempel zur Missbrauchsabwehr (Rate-Limiting, max. 30 Tage)

4. Kategorien betroffener Personen

• Endkundinnen und Endkunden des Salon-Kunden (Verbraucher im Sinne § 13 BGB)
• Beschäftigte des Salon-Kunden, sofern diese das Admin-Dashboard nutzen (Mitarbeiter-IDs, ggf. Login-Daten)

5. Pflichten des Auftragnehmers

(1) Verarbeitung der Daten ausschließlich im Rahmen der dokumentierten Weisungen des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO). Mündliche Weisungen werden unverzüglich schriftlich bestätigt.

(2) Sicherstellung, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(3) Umsetzung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO (siehe Anlage 1 - TOM).

(4) Unterstützung des Auftraggebers bei der Erfüllung der Betroffenenrechte (Art. 12-22 DSGVO) durch geeignete technische und organisatorische Maßnahmen.

(5) Unterstützung des Auftraggebers bei Datenschutz-Folgenabschätzungen (Art. 35, 36 DSGVO) und bei der Meldung von Datenschutzverletzungen (Art. 33, 34 DSGVO).

(6) Nach Abschluss der Erbringung der Verarbeitungsleistungen: Nach Wahl des Auftraggebers Löschung oder Rückgabe aller personenbezogenen Daten sowie Löschung vorhandener Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht (Art. 28 Abs. 3 lit. g DSGVO).

(7) [illegible] eines Ansprechpartners für [illegible] Datenschutzfragen [illegible] Marcus E[illegible] info[illegible]platrion[illegible].

(8) [illegible] des Verzeichnisses aller Verarbeitungstätigkeiten im Auftrag des Auftraggebers [illegible] Art. 30 Abs. 2 DSGVO.

(9) Bereitstellung aller erforderlichen Informationen zum Nachweis der Einhaltung dieser Verpflichtungen (Art. 28 Abs. 3 lit. h DSGVO) sowie Ermöglichung und Unterstützung von Audits durch den Auftraggeber oder einen von ihm beauftragten Prüfer (mit angemessener Vorankündigung, werktags).

(10) Unverzügliche Information des Auftraggebers, wenn nach Ansicht des Auftragnehmers eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt.

6. Unterauftragsverhältnisse (Subunternehmer)

(1) Der Auftraggeber erteilt hiermit die allgemeine schriftliche Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Subunternehmer) gemäß Art. 28 Abs. 2 DSGVO.

(2) Der Auftragnehmer setzt derzeit folgende Subunternehmer ein:

• Hosting-Provider (Rechenzentrum in Frankfurt am Main, Deutschland) - Server-Infrastruktur, ausschließlich EU/EWR
• Resend Ltd. (via EU-Endpoint) - transaktionaler Versand von Buchungsbestätigungen und Erinnerungsmails; Datenübermittlung in die USA nach EU-U.S. Data Privacy Framework (Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023)
• Stripe Payments Europe Ltd., Dublin, Irland - Kartenzahlung für die monatliche SaaS-Nutzungsgebühr (Auftragnehmer↔Salon-Kunde, keine Endkundendaten)

(3) Mit sämtlichen Subunternehmern, die personenbezogene Daten verarbeiten, bestehen entsprechende Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO bzw. Standardvertragsklauseln, soweit eine Übermittlung in Drittländer erfolgt.

(4) Der Auftragnehmer informiert den Auftraggeber rechtzeitig vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder den Austausch weiterer Auftragsverarbeiter. Der Auftraggeber kann der Änderung binnen 30 Tagen aus wichtigem Grund widersprechen.

7. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragnehmer hat die in Anlage 1 näher beschriebenen technischen und organisatorischen Maßnahmen getroffen und hält diese während der Vertragslaufzeit auf einem dem Stand der Technik entsprechenden Niveau.

8. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Sinne der DSGVO Verantwortlicher für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung insgesamt.

(2) Der Auftraggeber hat das Recht, sich jederzeit von der Einhaltung der getroffenen Maßnahmen zu überzeugen. Der Auftragnehmer wird nach vorheriger Terminabstimmung Einsicht in Dokumentationen und relevante Systeme gewähren. Umfangreiche Prüfungen werden nach Aufwand abgerechnet, soweit sie über eine jährliche Auskunft hinausgehen.

9. Meldung von Datenschutzverletzungen

(1) Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntnisnahme. Die Meldung enthält mindestens die in Art. 33 Abs. 3 DSGVO genannten Informationen.

(2) Der Auftraggeber bleibt für die Erfüllung seiner Meldepflicht gegenüber der Aufsichtsbehörde (72-Stunden-Frist) verantwortlich.

10. Rückgabe und Löschung von Daten

(1) Mit Beendigung der Leistungserbringung wird der Auftragnehmer auf Wahl des Auftraggebers die Daten entweder vollständig zurückgeben (z. B. als JSON/XLSX-Export) oder datenschutzkonform löschen.

(2) Die Löschung wird schriftlich bestätigt. Gesetzliche Aufbewahrungspflichten (insbesondere handels- und steuerrechtliche) bleiben unberührt; entsprechende Daten werden bis zum Ablauf der jeweiligen Fristen mit eingeschränkter Verarbeitung aufbewahrt.

11. Haftung

Die Haftung richtet sich nach den Regelungen des Hauptvertrags. Für Ansprüche Betroffener nach Art. 82 DSGVO gelten die dort getroffenen Bestimmungen.

12. Schlussbestimmungen

(1) Es gilt ausschließlich deutsches Recht. Gerichtsstand ist Reutlingen.

(2) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Änderung dieses Schriftformerfordernisses.

(4) Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV vor, soweit datenschutzrechtliche Belange betroffen sind.

Unterschriften

Ort, Datum, Unterschrift Auftraggeber (_____ (vom Salon-Kunden auszufüllen))	Dettingen an der Erms, 09.09.2026 - Marcus Euchner Auftragnehmer (Marcus Euchner, Platrion)

Anlage 1 - Technische und organisatorische Maßnahmen

gemäß Art. 32 DSGVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Zutrittskontrolle: Die Verarbeitung erfolgt ausschließlich in gesicherten Rechenzentren der Hosting-Provider mit kontrolliertem Zutritt, Videoüberwachung und Alarmanlagen.
• Zugangskontrolle: Zugriff auf Systeme ausschließlich per individuellem Login, starke Passwortrichtlinie, 2-Faktor-Authentifizierung für administrative Zugänge.
• Zugriffskontrolle: Rollen- und berechtigungsbasiertes Konzept, Minimalprinzip. Mandantenfähige Trennung auf Datenbankebene.
• Trennungskontrolle: Logische Trennung der Kundendaten pro Mandant. Produktions- und Entwicklungsumgebungen sind getrennt.
• Pseudonymisierung, soweit möglich; Verschlüsselung sensibler Felder.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

• Weitergabekontrolle: Datenübertragung ausschließlich verschlüsselt (TLS 1.2+).
• Eingabekontrolle: Protokollierung administrativer Änderungen in System-Logs.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Verfügbarkeitskontrolle: Redundante Infrastruktur, automatische Failover bei kritischen Komponenten, regelmäßige Sicherheitsupdates.
• Backup-Konzept: Tägliche automatische Backups der Datenbank, wöchentliche vollständige Backups, Aufbewahrung mindestens 7 Tage.
• Notfallplan: Dokumentierter Disaster-Recovery-Plan mit definierten Wiederherstellungszeiten.

Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

• Datenschutz-Management: Regelmäßige Selbstprüfung und Dokumentation der Verarbeitungstätigkeiten.
• Incident-Response-Management: Definierte Abläufe zur Meldung und Behandlung von Sicherheitsvorfällen innerhalb von 24 Stunden.
• Datenschutzfreundliche Voreinstellungen (Privacy by Default / by Design) gemäß Art. 25 DSGVO.
• Auftragskontrolle: Vertragliche Bindung aller Unterauftragsverarbeiter nach Art. 28 DSGVO.

Die vorgenannten Maßnahmen werden regelmäßig überprüft und dem Stand der Technik angepasst. Wesentliche Änderungen werden dem Auftraggeber in geeigneter Form mitgeteilt.